UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

CHIANTI PROSSER, individually and on behalf of all others similarly situated, Plaintiff, v. NEW YORK LIFE INSURANCE COMPANY, Defendant.	Civil Action No.: **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Chianti Prosser, individually and on behalf of all others similarly situated ("Class Members"), brings this action against Defendant New York Life Insurance Company ("Defendant"), alleging as follows based upon personal knowledge, information and belief, and investigation of counsel.

I. INTRODUCTION

1. This action arises from Defendant's unauthorized disclosure of the confidential personal information, Personally Identifying Information[1] ("PII") of Plaintiff and the millions of proposed Class Members via an October 2023 cyber attach on its information systems and Defendant's failure to reasonable mitigate against the foreseeability of such an attack. Because of Defendant's failures to implement reasonable, industry standard cyber security safeguards, Plaintiff and the Proposed Class Members have and will continue to suffer harm.

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

2. Because of Defendant's failures, the sensitive PII of Plaintiff and the Proposed Class was disclosed to a notorious cyber and identify theft gang, including Plaintiff's and Class Member's names and social security numbers (the "Data Breach").

3. Although Defendant discovered the Data Breach on November 2, 2023, Defendant failed to notify and warn Data Breach victims of the unauthorized disclosure of their PII until September 5, 2024, an egregious ten-month delay.

4. Plaintiff and Class Members are current and former insureds under life insurance and group benefit plans provided and/or serviced by Defendant. As a condition of obtaining insurance and/or benefit products and services, Plaintiff and Class Members were required to entrust their sensitive, non-public Private Information to Defendant.

5. Defendant contracted Infosys McCamish Systems, LLC ("IMS") to support and facilitate Defendant's operations and corporate functions and provided IMS the Private Information Defendant had collected from Plaintiff and Class Members. When the Data Breach occurred, Plaintiff's and Class Members' Private Information was maintained on IMS's network systems.

6. Businesses that handle consumers' Private Information like Defendant owe the individuals to whom the information relates a duty to adopt reasonable measures to protect it from disclosure to unauthorized third parties, and to keep it safe and confidential. This duty arises under contract, statutory and common law, industry standards, representations made to Plaintiff and Class Members, and because it is foreseeable that the exposure of Private Information to unauthorized persons—and especially hackers with nefarious intentions—will harm the affected individuals, including but not limited to the invasion of their private health and financial matters.

7. Defendant breached its duties owed to Plaintiff and Class Members by failing to

safeguard the Private Information that it collected and maintained, including by failing to reasonably supervise its vendor's cybersecurity practices, which allowed criminal hackers to access and steal at least thousands of individuals' Private Information in the Data Breach.

8. According to the September 5, 2024, notice sent by IMS on Defendant's behalf to victims of the Data Breach ("Notice Letter"), on or about November 2, 2023, IMS "became aware that certain IMS systems were encrypted by ransomware." The ensuing investigation revealed that between October 29 and November 2, 2023, "data was subject to unauthorized access and acquisition," including full names and Social Security numbers of Defendant's customers.

9. Plaintiff has now learned that the cyber gang LockBit was behind the Data Breach and has published Plaintiff's and Class Members' stolen Private Information to its dark web leak site, exposing it to an untold number of bad actors with nefarious intentions for years to come.

10. Defendant breached its duties and obligations by failing in one or more of the following ways: (a) to ensure its vendor designed, implemented, monitored, and maintained reasonable network safeguards against foreseeable threats; (b) to design, implement, and maintain reasonable data retention policies; (c) to adequately train or oversee staff and service providers regarding data security; (d) to comply with industry-standard data security practices; (e) to warn Plaintiff and Class Members of the inadequate data security practices of Defendant's vendors collecting their Private Information; (f) to encrypt or adequately encrypt the Private Information, or ensure its vendor did so; (g) to ensure its vendor handling Private Information had industry-standard and legally compliant data security to protect it; (h) to recognize or detect that IMS's network had been compromised and accessed in a timely manner to mitigate the harm; (i) to utilize, or to ensure its vendor utilized, widely available software able to detect and prevent this type of attack; (j) and to otherwise secure the Private Information using reasonable and effective data

security procedures free of foreseeable vulnerabilities and data security incidents.

11. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality and security of their Private Information. In providing their Private Information to Defendant, Plaintiff and the Class Members reasonably expected this sophisticated business entity to keep their Private Information confidential and security maintained, to use it for business purposes, and to disclose it only as authorized. Defendant failed to do so, resulting in the unauthorized disclosure of Plaintiff's and Class Members' Private Information in the Data Breach.

12. LockBit targeted and obtained Plaintiff's and Class Members' Private Information from Defendant because of the data's value in exploiting and stealing Plaintiff's and Class Members' identities. As a direct and proximate result of Defendant's inadequate data security and breaches of its duties to handle Private Information with reasonable care, Plaintiff's and Class Members' Private Information was accessed by cybercriminals and has now been exposed to an untold number more. The present and continuing risk to Plaintiff and Class Members as victims of the Data Breach will remain for their respective lifetimes.

13. The harm resulting from a cyberattack like this Data Breach manifests in numerous ways including identity theft and financial fraud, and the exposure of a Private Information in a breach ensures that the subject individual will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of his or her life. Mitigating that risk, to the extent even possible, requires individuals to devote significant time and money to closely monitor their credit, financial accounts, and email accounts, and take several additional prophylactic measures.

14. The risk of identity theft caused by this Data Breach is impending and has materialized, as Plaintiff's and Class Members' Private Information was targeted, accessed,

misused, and has already been published and disseminated on the LockBit dark web leak site.

15. To make matters worse, although IMS confirmed the Data Breach's occurrence by November 2, 2023, Defendant until September 5, 2024—*nearly a year* after the Data Breach happened—that their Private Information had been compromised, diminishing Plaintiff's and Class Members' ability to timely and thoroughly mitigate and address harms resulting from the Data Breach.

16. As a result of the Data Breach, Plaintiff and Class Members, suffered concrete injuries in fact including but not limited to (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) actual identity theft and fraud; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) deprivation of value of their Private Information; (g) loss of privacy; (h) emotional distress including anxiety and stress in with dealing with the Data Breach; and (i) the continued risk to their sensitive Private Information, which remains in Defendant's possession and control and subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect the customer data it collects and maintains.

17. To recover for these harms, Plaintiff, on behalf of herself and the Class as defined herein, brings claims for negligence/negligence *per se*, breach of implied contract, violations of New York General Business Law, and unjust enrichment to address Defendant's inadequate safeguarding of Plaintiff's and Class Members' Private Information in its custody, and Defendant's failure to provide timely or adequate notice to Plaintiff and Class Members that their information was compromised in the Data Breach.

18. Plaintiff and Class Members seek compensatory, nominal, statutory, and punitive

damages, declaratory judgment, and injunctive relief requiring Defendant to (a) disclose, expeditiously, the full nature of the Data Breach and the types of Private Information exposed; (b) implement improved data security practices to reasonably guard against future breaches of Private Information in Defendant's and its vendors' possessions; and (c) provide, at Defendant's own expense, all impacted Data Breach victims with lifetime identity theft protection services.

II. THE PARTIES

19. Plaintiff Chianti Prosser is a citizen and resident of the State of South Carolina, and resides in North Charleston, where she intends to stay.

20. At all relevant times, Plaintiff received insurance and/or benefit products and services from Defendant. As a condition of and in exchange for her receipt of Defendant's products and services, Plaintiff was required to, and did, provide her Private Information to Defendant, and through Defendant, to IMS.

21. Defendant New York Life Insurance Company is a New York corporation with its principal place of business located at 51 Madison Ave, New York, NY 10010.

22. Defendant, who is "the largest mutual insurer in the U.S.,"[2] reported $329.5 billion in cash and assets in 2023 and nearly $32 billion in statutory surplus and Asset Valuation Reserve.[3]

III. JURISDICTION AND VENUE

23. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because the amount in controversy exceeds $5 million, exclusive of interest and costs, and the number of Class Members exceeds 100, many of whom (namely, Plaintiff) have different citizenship from Defendant.

24. This Court has personal jurisdiction over Defendant because it is incorporated and

[2] https://www.newyorklife.com/
[3] https://www.newyorklife.com/assets/docs/pdfs/nyl-internet/file-types/2023-nyl-investment-report.pdf

headquartered in New York and engaged in substantial and not isolated activity in New York.

25. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant operates in this District and a substantial part of the events or omissions giving rise to Plaintiff's and Class Members' claims occurred in this District, including Defendant's collecting and/or failing to secure Plaintiff's and Class Members' Private Information.

IV. GENERAL FACTUAL ALLEGATIONS

A. Defendant's Data Breach

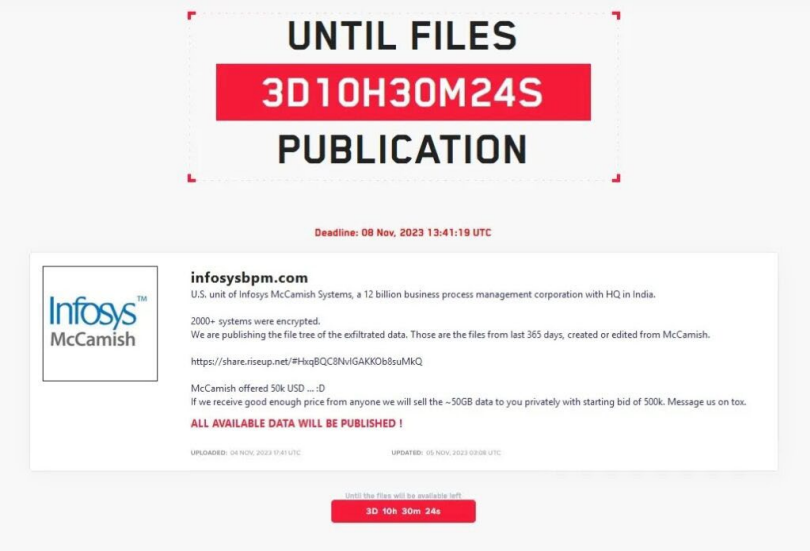
26. Around October 29, 2023, Defendant was attacked by "one of the most high-profile ransomware gangs ever," Lockbit, which targets multi-billion-dollar businesses like Defendant.[4]

27. Apparently before Defendant even noticed that its information systems had been breached, the attackers had time to perform reconnaissance of Defendant's digital assets, identity documents containing Plaintiff's and Class Members PII, and exfiltrate that data, over the course of five days.

28. Had Defendant implemented industry standard logging, monitoring, and alerting procedures and technology, Defendant could have prevented this exfiltration.

29. Instead, the Lockbit group was able to steal value data, including social security numbers, which it then posted for sale on the dark web via its leak site, which is where such cyber gangs often post sample data after their targets refuse to timely pay the ransom. Lockbit announced that it would sell the data at a starting bid of $500,000:[5]

[4] https://www.comparitech.com/news/infosys-notifies-6-million-people-about-data-breach-claimed-by-lockbit-ransomware-gang/
#:~:text=IT%20consulting%20company%20Infosys%20yesterday%20confirmed%20it
[5] *Id.*



30. In all, Lockbit is believed to have stolen at least 50 GB of data that it selected from Defendant's information systems.[6]

B. Defendant New York Life Insurance Company

31. Defendant is an insurance and benefit company and contracted with IMS to provide administrative services to Defendant's Group Benefits division's corporate and business market operations.

32. As part of and to facilitate its business, Defendant collects and maintains the Private Information of millions of its current and former customer-insureds, including Plaintiff and Class Members.

33. As a condition and in exchange for receiving insurance and/or benefit products and services, Plaintiff and Class Members were required to entrust their highly sensitive Private Information to Defendant.

34. Defendant derived economic benefits from collecting Plaintiff's and Class Members' Private Information. Without the required submission of Private Information,

[6] *Id.*

Defendant could not perform its operations, furnish its products and services, or generate its revenue.

35. To operate its business and facilitate IMS's contracted support services, Defendant provided Plaintiff's and Class Members' Private Information to IMS.

36. At all relevant times, Defendant knew IMS was storing and using its networks to store and transmit valuable, sensitive Private Information belonging to Plaintiff and Class Members, and that as a result, IMS's systems would be attractive targets for cybercriminals.

37. Defendant also knew that any breach of IMS's information technology network and exposure of the data stored therein would result in the increased risk of identity theft and fraud for the millions of individuals whose Private Information was compromised, as well as intrusion into those individuals' private and sensitive personal matters.

38. In exchange for receiving Plaintiff's and Class Members' Private Information, Defendant promised to safeguard the sensitive, confidential data and ensure it was used only for authorized and legitimate purposes, to delete such information once there was no longer a need to maintain it, and to ensure the same practices from its vendors handling the Private Information, including IMS.

39. Indeed, Defendant's Privacy Notice, published on its website, affirms and warrants in part as follows:

> **Safeguarding your information**
> We maintain physical, electronic, and procedural safeguards that meet state and federal regulations. Access to customer information is limited to people who need the information to perform their job responsibilities. We regularly update and improve our security standards, procedures, and technology to protect against unauthorized access to your confidential information. [7]

[7] Privacy Notice, New York Life Group Benefit Solutions, Sept. 2023, available at https://www.newyorklife.com/group-benefit-solutions/privacy-notice.

40. Defendant's Privacy Notice further promises that the Private Information it collects will be used "as allowed by law," including a list of specific circumstances —none of which are exposure to cybercriminals in a data breach.[8]

41. Upon information and belief, Defendant provided the foregoing privacy notices and policies to all customers receiving insurance and/or benefit products and services from Defendant, including Plaintiff and Class M As part of its business, Defendant collects, uses, and controls millions of individuals' Private Information, including that of Plaintiff and Class Members.

C. Plaintiff Prosser

42. Plaintiff Prosser, a former insured of Defendant, received a data breach notification letter form Defendant on September 5, 2024 from IMS on behalf of Defendant. Exhibit A.

43. As a condition of obtaining insurance and/or benefit products and services, Plaintiff was required to entrust her sensitive, non-public Private Information to Defendant. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties, including her name, employee ID, personal address, client or customer account number/policy number, Social Security number, date of birth, and financial account number.

44. At the time of the Data Breach—October 29, 2023 through November 2, 2023—Defendant maintained Plaintiffs Private Information in its system.

45. Plaintiff is very careful about sharing her sensitive Private Information. She stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other

[8] *Id.*

unsecured source. Plaintiff would not have entrusted her Private Information to Defendant had she known of Defendant's lax data security policies.

46. The letter failed to include any information regarding the source of the attack or any specific information on what Defendant was doing to prevent such an attack from happening again.

47. The letter failed to notify Plaintiff that some of the stolen information had already appeared on the dark web.

48. Notwithstanding that the letter claimed that Defendant cares about Plaintiff's information, Defendant offered Plaintiff only twenty-four months of credit monitoring services, which is woefully inadequate to redress the harms caused by Defendant's failures.

49. Because of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

50. The need to spend this time was not speculative because Plaintiff was merely performing the tasks that Defendant told her she could take to help protect her personal information, which Plaintiff believed—and still believes—was necessary given the instructions in Defendant's notification letter.

51. Furthermore, the time spent mitigating the effects of Defendant's failures was more significant because Defendant failed to timely information Plaintiff of the Breach, thus requiring Plaintiff to review more account information for fraudulent activity.

52. Plaintiff's and the proposed Class Members' PII was provided to Defendant with

the reasonable expectation and mutual understanding that Defendant would comply with their obligations to keep such information confidential and secure from unauthorized access. By failing to do so, Defendant put all Class Members at risk of identity theft, financial fraud, and other harms and caused Plaintiff and Class Members to have to spend their own valuable time responding to Defendant's failures.

53. Plaintiff has suffered actual injury from having her Private Information compromised because of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

54. Moreover, Defendant's failures have now left Plaintiff and Class Members to deal with the anxiety and stress that is inherent in data breaches, especially those that expose individuals' social security numbers.

55. Plaintiff additionally suffered actual injury in the form of her Private Information being disseminated on the dark web, which, upon information and belief, was caused by the Data Breach.

56. Plaintiff additionally suffered actual injury in the form of experiencing an increase

in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of her Private Information was caused, upon information and belief, by the fact that cybercriminals can easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

57. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

58. Because of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

59. Because of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

60. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches, which are highly likely to occur unless Defendant substantially improves its cybersecurity systems.

D. Defendant Failed to Adequately Safeguard Plaintiff's and Class Member's Private Information, resulting in the Data Breach.

61. Defendant had and continues to have duties to adopt reasonable measures to keep Plaintiff's and Class Members' Private Information confidential and protected from disclosure to unauthorized third parties, and to audit, monitor, and verify the integrity of its IT networks and

those of their vendors and affiliates.

62. Defendant's obligations stem from the Federal Trade Commission ("FTC") Act, 15 U.S.C. § 45, common law, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and protected from unauthorized disclosure.

63. Plaintiff and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information. To that end, Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

64. Based on the foregoing representations and warranties and to obtain insurance and/or benefit products and services from Defendant, directly or indirectly, Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its promises and obligations to keep such information confidential and protected against unauthorized access.

65. Plaintiff and Class Members relied on these promises from Defendant, and but for Defendant's promises to keep Plaintiff's and Class Members' Private Information secure and confidential, would not have sought services from or entrusted their Private Information to Defendant. Consumers, in general, demand security for their Private Information, especially when Social Security numbers and other sensitive data are involved.

66. Additionally, by obtaining, using, and benefitting from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting that Private Information from unauthorized access and disclosure.

67. Defendant's duty to protect Plaintiff and Class Members from the foreseeable risk

of injury that inadequate data protection and unauthorized exposure of their Private Information would case obligated Defendant to implement reasonable practices to keep Plaintiff's and Class Members' sensitive Private Information confidential and securely maintained, to use and disclose it for necessary and authorized purposes only, to ensure it was deleted from its and its vendors' network systems when no longer necessary for legitimate business purposes, and to ensure the same data security protocols and procedures from its vendor IMS. Defendant failed to do so.

68. On or about September 5, 2024—*nearly a year* after the Data Breach—IMS, on Defendant's behalf, began sending Plaintiff and other Data Breach victims the Notice Letter titled "Notice of Data Breach."

69. Despite its direct insurer-insured relationship with Plaintiff and Class Members, Defendant did not send separate notifications to its customers impacted by the Data Breach, relying solely on IMS's Notice Letters to alert Data Breach victims.

70. The Notice Letters generally inform as follows:

> Infosys McCamish Systems, LLC ("IMS") writes to inform you of an incident that involved some of your personal information. IMS supports New York Life Group Benefit Solutions' corporate and business market operations, such as administering group benefits and/or sending benefit communication letters.
>
> * * *
>
> **WHAT HAPPENED?** On November 2, 2923, IMS became aware that certain IMS systems were encrypted by ransomware (the "Incident"). . . . The in-depth cyber forensic investigation determined that unauthorized activity occurred between October 19, 2023, and November 2, 2023. Through the investigation, it was also determined that data was subject to unauthorized access and acquisition. . . . After a comprehensive review, it was determined that some of your personal information was subject to unauthorized access/acquisition.
>
> **WHAT INFORMATION WAS INVOLVED?** The investigation determined that the following types of your personal information

were involved: your name and Social Security number.[9]

71. Omitted from the Notice Letters are crucial details like the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information is protected.

72. The Notice Letters also fail to disclose that the notorious LockBit hacker group had claimed responsibility for the Data Breach, or that LockBit had published the trove of stolen Private Information on its dark web leak site for any number of unknown and nefarious actors to take and further misuse.

73. Thus, Defendant's purported disclosure amounts to no real disclosure at all, as it fails to inform Plaintiff and Class Members of the Data Breach's critical facts with any degree of specificity. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach was and is severely diminished.

74. LockBit has now published the Private Information stolen in the Data Breach on its dark web leak site, including Defendant's customers' full names and Social Security numbers. Upon information and belief, the Private Information has already been viewed on LockBit's dark web site thousands of times, if not more.

75. Upon information and belief, LockBit first breached IMS's network and exfiltrated Plaintiff's and Class Members' Private Information stored in un-encrypted form therein, then encrypted IMS systems once the Private Information was exfiltrated, dropping a ransom note during encryption.

[9] Exhibit A, Data Breach Notification Letter to Plaintiff.

76. Defendant could have prevented this Data Breach by requiring IMS to implement such reasonable safeguards as properly securing, sanitizing, and encrypting the files and servers containing Plaintiff's and Class Members' Private Information, and by supervising IMS's data security during the course of its contracts with Defendant to ensure such reasonable safeguards were continuously maintained, but failed to do so.

77. For example, if Defendant had ensured that IMS implemented industry standard logging, monitoring, and alerting systems—basic technical safeguards that any PII-collecting company is expected to employ—then cybercriminals would not have been able to perpetrate prolonged malicious activity in IMS's network systems without alarm bells going off, including the reconnaissance necessary to identify where PII was stored, installation of malware or other methods of establishing persistence and creating a path to exfiltrate data, staging data in preparation for exfiltration, and then exfiltrating that data outside of IMS's system without being caught.

78. Had Defendant required, by contract and oversight, that IMS implement basic monitoring and detection systems, IMS would have recognized the malicious activities detailed in the preceding paragraph, which then would have stopped the Data Breach or greatly reduced its impact.

79. Defendant did not use reasonable security procedures and practices appropriate to the sensitive and confidential nature of Plaintiff's and Class Members' Private Information it collected and shared with vendors, including IMS, such as requiring its vendors to encrypt files containing Private Information and delete Private Information from network systems when it is no longer needed, which caused that Private Information's unauthorized access and exfiltration in the Data Breach.

80. Defendant's tortious conduct and breach of contractual obligations, as detailed in

this Complaint, are evidenced by its failure to recognize the Data Breach or its impacts on Defendant's customers until months after cybercriminals had breached IMS network and accessed Plaintiff's and Class Members' Private Information stored therein—meaning Defendant had no effective means in place to ensure that cyberattacks of its vendors storing Private Information were detected and prevented.

E. Defendant Knew of the Risk of a Cyberattack because Businesses in Possession of Private Information are Particularly Suspectable.

81. Defendant's negligence in failing to safeguard Plaintiff's and Class Members' Private Information is exacerbated by the repeated warnings and alerts regarding the need to protect and secure sensitive data.

82. Private Information of the kind accessed in the Data Breach is of great value to cybercriminals as it can be used for a variety of unlawful and nefarious purposes, including ransomware, fraudulent misuse, and sale on the internet black market known as the dark web.

83. Private Information can also be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and financial records. This may be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, like his or her birthdate, birthplace, or mother's maiden name.

84. Data thieves regularly target businesses in the healthcare and insurance industries like Defendant due to the highly sensitive information that such entities maintain. Defendant knew and understood that unprotected Private Information is highly sought after by criminals who seek to illegally monetize that Private Information through unauthorized access.

85. Cyber-attacks against institutions such as Defendant and its vendor IMS are targeted and frequent. According to Contrast Security's 2023 report *Cyber Bank Heists: Threats to the financial sector*, "Over the past year, attacks have included banking trojans, ransomware,

account takeover, theft of client data and cybercrime cartels deploying 'trojanized' finance apps to deliver malware in spear-phishing campaigns."[10] In fact, "40% [of financial institutions] have been victimized by a ransomware attack."[11]

86. In light of past high profile data breaches at industry-leading companies, including, for example, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or, if acting as a reasonable business handling PII, should have known that the Private Information it collected, used, and shared with IMS would be vulnerable to and targeted by cybercriminals.

87. According to the Identity Theft Resource Center's report covering the year 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017."[12]

88. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant itself. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[13]

---

[10] Contrast Security, "Cyber Bank Heists: Threats to the financial sector," pg. 5, avail. at https://www.contrastsecurity.com/hubfs/Cyber%20Bank%20Heists%20Report%202023.pdf?hsLang=en (last visited Aug. 22, 2024).

[11] *Id.*, at 15.

[12] *See* "Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises," ITRC, Jan. 24, 2022, available at https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/ (last visited Aug. 22, 2024).

[13] IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at https://www.ibm.com/reports/data-breach (last accessed Feb. 9, 2024).

89. Indeed, Defendant's other service provider had recently experienced a cyberattack that exposed customer PII, just months before this Data Breach. Thus, Defendant was acutely aware of the risk of a data breach and the harm that a vendor's inadequate data security measures would cause.

90. Defendant's data security obligations were particularly important given the substantial increase, preceding the date of the subject Data Breach, in cyberattacks and/or data breaches targeting entities like Defendant and its vendors that collect and store PII.

91. In 2023, an all-time high for data compromises occurred, with 3,205 compromises affecting 353,027,892 total victims. Of the 3,205 recorded data compromises, 809 of them, or 25.2% were in the medical or healthcare industry. The estimated number of organizations impacted by data compromises has increased by +2,600 percentage points since 2018, and the estimated number of victims has increased by +1400 percentage points. The 2023 compromises represent a 78 percentage point increase over the previous year and a 72 percentage point hike from the previous all-time high number of compromises (1,860) set in 2021.

92. As a business in possession of customers' Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class Members and of the foreseeable consequences if Defendant's or its vendor's network systems were breached. Such consequences include the significant costs imposed on Plaintiff and Class Members due to a breach. Nevertheless, Defendant failed to implement or follow reasonable cybersecurity measures to protect against the Data Breach.

93. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

94. Given the nature of the Data Breach, it was foreseeable that Plaintiff's and Class Members' Private Information compromised therein would be targeted by hackers and cybercriminals for use in variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiff's and Class Members' Private Information can easily obtain their tax returns or open fraudulent credit card accounts in Plaintiff's and Class Members' names.

95. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on IMS's network server(s), amounting to at least thousands of individuals' detailed Private Information, and, thus, that these individuals would be harmed by the exposure of that unencrypted data.

96. Plaintiff and Class Members were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting, using, and sharing Private Information and the critical importance of providing adequate security for that information.

97. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiff and Class Members especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and the like.

F. Defendant was Required, But Failed to Comply with FTC Rules and Guidance.

98. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

99. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-

making.

100. In 2016, the FTC updated its publication, *Protecting PII: A Guide for Business*, which establishes cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[14]

101. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[15]

102. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take

[14] *See* Federal Trade Commission, *Protecting Private information: A Guide for Business* (October 2016), https://www.bulkorder.ftc.gov/system/files/publications/2_9-00006_716a_protectingpersinfo-508.pdf.
[15] *See id*.

to meet their data security obligations.

103. These FTC enforcement actions include actions against entities failing to safeguard PII such as Defendant. *See, e.g.*, *In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

104. Defendant failed to properly implement basic data security practices widely known throughout the industry. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

105. Defendant was always fully aware of its obligations to protect the PII of Plaintiff and the Class Members. Defendant was also aware of the significant repercussions that would result from its failure to do so.

106. For example, the FTC notes that companies should maintain central log files, monitor incoming traffic for signs of malicious attempts and activity, and monitoring outgoing traffic to identify signs of data exfiltration.[16] If Defendant had these controls in place, it would have realized that cybercriminals had infiltrated its systems, were performing reconnaissance to identify valuable data, and it likely would have realized that the data was being exfiltrated before it was too late.

107. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards.

108. The Center for Internet Security's (CIS) CIS Critical Security Controls (CSC)

[16] *Id.* at pp. 21–22.

recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including 18 Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[17]

109. In addition, the National Institute of Standards and Technology (NIST) recommends certain practices to safeguard systems, *infra,* such as:

- Control who logs on to your network and uses your computers and other devices.
- Use security software to protect data.
- Encrypt sensitive data, at rest and in transit.
- Conduct regular backups of data.
- Update security software regularly, automating those updates if possible.
- Have formal policies for safely disposing of electronic files and old devices.
- Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.[18]

110. Further still, the Cybersecurity & Infrastructure Security Agency makes specific

[17] *See* Rapid7, *CIS Top 18 Critical Security Controls Solutions*, https://www.rapid7.com/solutions/compliance/critical-controls (last accessed July 11, 2024).
[18] Federal Trade Commission, *Understanding the NIST Cybersecurity Framework*, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework (last accessed July 11, 2024).

recommendations to organizations to guard against cybersecurity attacks, including (1) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to theorganization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (2) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (3) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[19]

111. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, as well as failing to comply with other industry standards for protecting Plaintiff's and the proposed Class Members' PII, resulting in the Data Breach.

[19] Cybersecurity & Infrastructure Security Agency, *Shields Up: Guidance for Organizations*, https://www.cisa.gov/shields-guidance-organizations (last accessed July 11, 2024).

G. Defendant Failed to Comply with Industry Standards.

112. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards.

113. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.

114. In addition, the NIST recommends certain practices to safeguard systems, *infra*, such as the following:

a. Control who logs on to your network and uses your computers and other devices.

b. Use security software to protect data.

c. Encrypt sensitive data, at rest and in transit.

d. Conduct regular backups of data.

e. Update security software regularly, automating those updates if possible.

f. Have formal policies for safely disposing of electronic files and old devices; and

g. Train everyone who uses your computers, devices, and network about cybersecurity.

115. Further still, the Cybersecurity & Infrastructure Security Agency makes specific recommendations to organizations to guard against cyberattacks, including (a) reducing the

likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior, [e]nabl[ing] logging in order to better investigate issues or events[,] and [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated"; (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and; (d) other steps.[20]

116. Upon information and belief, Defendant failed to require, by contract or oversight, that IMS implement and maintain industry-standard cybersecurity measures, including the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, as well as other industry standards for protecting Plaintiff's and Class Members' Private Information, resulting in the Data Breach.

H. Defendant Owed Plaintiff and Class Members Common Law Duties to Safeguard their Private Information.

117. In addition to its obligations under federal and state laws, Defendant owed a duty

[20] Cybersecurity & Infrastructure Security Agency, "Shields Up: Guidance for Organizations," available at https://www.cisa.gov/shields-guidance-organizations (last visited Feb. 9, 2024).

to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its and/or its vendors' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. These duties owed to Plaintiff and Class Members obligated Defendant to (a) provide reasonable data security consistent with industry standards and requirements to protect Plaintiff's and Class Members' Private Information in its care and its vendor's custody from unauthorized disclosure, and (b) ensure its vendor IMS implemented and maintained such appropriate safeguards with respect to Plaintiff's and Class Members' Private Information.

118. Defendant owed duties to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in its and/or their vendors' possession, including adequately training employees and others who accessed Private Information on how to adequately protect Private Information.

119. Defendant owed duties to Plaintiff and Class Members to implement processes that would detect a compromise of Private Information in a timely manner.

120. Defendant owed duties to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

121. Defendant owed duties to Plaintiff and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

122. Defendant owed duties to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

123. Defendant failed to take the necessary precautions to safeguard and protect Plaintiff's and Class Members' Private Information from unauthorized disclosure. Defendant's actions and omissions represent a flagrant disregard of Plaintiff's and Class Members' rights.

124. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus, Defendant knew that failing to take reasonable steps to secure the Private Information, including ensuring its vendors implemented industry-standard and legally compliant security for PII, left the Private Information in a dangerous condition.

125. Indeed, just months prior to this Data Breach Defendant was involved in a cybersecurity incident targeted at one of Defendant's service providers, wherein a ransomware group accessed and filtrated Defendant's customers' PII. Thus, Defendant was fully aware of the need for and importance of performing due diligence and oversight of its vendors' data security policies and processes to ensure they were sufficient to protect the Private Information entrusted to Defendant.

126. Defendant failed to adequately protect Plaintiff's and Class Members' Private Information—and failed to even encrypt or redact this highly sensitive data, or ensure the same from its vendor that received, handled, and stored it. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect Plaintiff's and Class Members' sensitive data.

I. Plaintiff and Class Members Suffered Common Injuries and Damages due to Defendant's Conduct.

127. Defendant's failure to implement or maintain adequate data security measures for Plaintiff's and Class Members' Private Information directly and proximately caused injuries to Plaintiff and Class Members by the resulting disclosure of their Private Information in the Data Breach.

128. The ramifications of Defendant's failures to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen

fraudulent use of that information and damage to victims may continue for years.

129. Plaintiff and Class Members are also at a continued risk because their Private Information remains in Defendant's care, which has already been shown insufficient to protect customer information and leaves such data subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its customers' Private Information.

130. As a result of Defendant's ineffective and inadequate data security practices, the consequential Data Breach, and the foreseeable outcome of Plaintiff's and Class Members' Private Information ending up in criminals' possession, all Plaintiff and Class Members have suffered and will continue to suffer the following actual injuries and damages, without limitation: (a) invasion of privacy; (b) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) deprivation of value of their Private Information; (g) loss of the benefit of their bargain with Defendant; (h) emotional distress including anxiety and stress in dealing with the Data Breach's aftermath; and (i) the continued risk to their sensitive Private Information, which remains in Defendant's possession and control and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information it collects, uses, and shares.

Present and Ongoing Risk of Identity Theft

131. Plaintiff and Class Members are at a heightened risk of identity theft for years to come because of the Data Breach.

132. The FTC defines identity theft as "a fraud committed or attempted using the

identifying information of another person without authority."[21] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[22]

133. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the internet black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

134. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[23] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[24] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

135. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, and PII like the Private Information at issue here.[25]

---

[21] 17 C.F.R. § 248.201 (2013).
[22] *Id.*
[23] *What Is the dark web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[24] *Id.*
[25] *What is the dark web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

The digital character of Private Information stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[26] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[27]

136. The unencrypted Private Information of Plaintiff and Class Members has ***already*** been posted on LockBit's dark web leak site.

137. In addition, unencrypted and detailed Private Information may fall into the hands of companies that will use it for targeted marketing without the approval of Plaintiff and Class Members.

138. Unauthorized actors can easily access and misuse Plaintiff's and Class Members' Private Information due to the Data Breach.

139. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or to track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

140. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a

[26] *Id.; What Is the dark web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[27] *What is the dark web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

141. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[28]

142. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

143. Even then, new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that

[28] Social Security Administration, *Identity Theft and Your Social Security Number*, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

old bad information is quickly inherited into the new Social Security number."[29]

144. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for credit lines.[30]

145. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[31]

146. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an

---

[29] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Sep. 12, 2024).

[30] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), available at https://www.ssa.gov/pubs/EN-05-10064.pdf.

[31] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm (last visited Feb. 26, 2024).

astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

147. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

148. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

149. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

150. The development of "Fullz" packages means that stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. That is exactly what is happening to Plaintiff and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that their stolen Private Information is being misused, and that such misuse is traceable to the Data Breach.

151. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice,

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were

> reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.[32]

152. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[33]

153. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[34] Yet, Defendant failed to rapidly report to Plaintiff and Class Members that their Private Information was stolen.

154. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

155. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their Private Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

156. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Private Information. To protect themselves, Plaintiff

[32] Erika Harrell, *Bureau of Just. Stat.*, U.S. DEP'T OF JUST., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed Jan. 23, 2024).
[33] *See* https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.
[34] *Id.*

and Class Members will need to remain vigilant for years or even decades to come.

Loss of Time to Mitigate the Risk of Identify Theft and Fraud

157. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet the asset of time has been lost.

158. In the event that Plaintiff and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record

159. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must monitor their financial accounts for many years to mitigate that harm.

160. Plaintiff and Class Members have spent time, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover.

161. These efforts are consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports,

contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[35]

162. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendant's conduct that caused the Data Breach.

Diminished Value of Private Information

163. Private Information is a valuable property right.[36] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

164. For example, drug and medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase Private Information on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

165. Private Information can sell for as much as $363 per record according to the Infosec Institute.[37]

---

[35] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited Feb. 26, 2024).

[36] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PRIVATE INFORMATION") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PRIVATE INFORMATION, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[37] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

166. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[38] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[39] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[40]

167. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and likely release onto the dark web, where holds significant value for the threat actors.

168. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

Future Cost of Credit and Identify Theft Monitoring is Reasonable and Necessary

169. To date, Defendant has done nothing to provide Plaintiff and Class Members with relief for the damages they have suffered due to the Data Breach. Defendant, which had a direct relationship with Plaintiff and Class Members, did not offer Data Breach victims even minimal compensation like temporary complimentary credit monitoring services, or even bother to notify its customers of their Private Information's unauthorized exposure in the Data Breach.

---

[38] Lazarus, D., *Shadowy data brokers make the most of their invisibility cloak*, LA TIMES (Nov. 5, 2019), available at https://www.latimes.com/business/story/2019-11-05/column-data-brokers.
[39] https://datacoup.com/.
[40] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

170. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information, and the fact that LockBit has already published the stolen Private Information on its dark web, there is a strong probability that the Private Information will be further published and on the black market/dark web for sale and purchase by criminals intending to utilize the it for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money, filing false tax returns, taking out loans or lines of credit, or filing false unemployment claims.

171. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that her or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

172. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[41] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

173. Consequently, Plaintiff and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future, if not forever.

174. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members

[41] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The dark web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

from the risk of identity theft that arose from the Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

Loss of Benefit of the Bargain

175. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain.

176. When agreeing to provide their Private Information, which was a condition precedent to obtain insurance and related services from Defendant, and paying Defendant, directly or indirectly, for these products and services, Plaintiff and Class Members as consumers understood and expected that they were, in part, paying a premium for services and data security to protect the Private Information they were required to provide.

177. In fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains struck with Defendant.

V. CLASS ACTION ALLEGATIONS

178. Plaintiff bring this nationwide class action on behalf of herself and others similarly situated pursuant to Federal Rule of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4).

179. Plaintiff proposes the following nationwide class definition, subject to amendment based on information obtained through discovery:

> All persons in the United States whose Private Information was provided to Defendant and compromised in the Data Breach, including all persons who received a Notice Letter sent on Defendant's behalf ("Class").

180. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which

Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

181. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

182. **Numerosity:** The Class is so numerous that joinder of all members is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, upon information and belief, and according to Defendant's filings, a staggering 6.5 million individuals were affected,[42] making joinder of all members of the Class impractical.

183. **Commonality:** Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;

c. Whether Defendant had a duty not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

d. Whether Defendant had a duty not to use the Private Information of Plaintiff and Class Members for non-business purposes;

e. Whether Defendant had a duty to supervise its vendors' data security for Private

[42] https://www.infosys.com/investors/documents/update-mccamish-cybersecurity-incident.pdf

Information;

f. Whether Defendant knew or should have known of the data security vulnerabilities that allowed the Data Breach to occur;

g. Whether Defendant knew or should have known of the risks to Plaintiff's and Class Members' Private Information in IMS's custody;

h. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;

i. When Defendant actually learned of the Data Breach;

j. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members their Private Information had been compromised;

k. Whether Defendant violated data breach notification laws by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

l. Whether Defendant's conduct violated the FTC Act;

m. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

n. Whether Defendant and/or IMS adequately addressed and remedied the vulnerabilities that permitted the Data Breach to occur;

o. Whether Defendant engaged in unfair, unlawful, or deceptive practice by failing to safeguard the Private Information of Plaintiff and Class Members;

p. Whether Defendant engaged in unfair, unlawful, or deceptive practice by concealing and/or misrepresenting its and its vendors' data security processes and vulnerabilities;

q. Whether Defendant were unjustly enriched by failing to provide adequate security for

Plaintiff's and Class Members' Private Information;

r. Whether Plaintiff and Class Members are entitled to actual, consequential, nominal, statutory, and/or punitive damages as a result of Defendant's wrongful conduct;

s. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

t. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm the Data Breach caused.

184. **Typicality:** Plaintiff's claims are typical of other Class Members' claims because Plaintiff and Class Members were subject to the same unlawful conduct as alleged herein, and were damaged in the same way. Plaintiff's Private Information provided to Defendant and through Defendant, to IMS, and was compromised due to the Data Breach. Plaintiff's damages and injuries are akin to those of other Class Members and Plaintiff seeks relief consistent with the relief of the Class.

185. **Adequacy:** Plaintiff is an adequate representative of the Class because he is a member of the Nationwide Class and committed to pursuing this matter against Defendant to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the interests of the Class.

186. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to Plaintiff and Class Members may not be

sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and Class Members are relatively small compared to the burden and expense required to individually litigate their claims against Defendant, and thus, individual litigation to redress Defendant's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

187. **Manageability:** The litigation of the class claims alleged herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates there would be no significant manageability problems with prosecuting this lawsuit as a class action. Adequate notice can be given to Class Members directly using information maintained in Defendant's and/or IMS's records.

188. **Ascertainability:** All members of the proposed Class are readily ascertainable. The Class is defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the Class. Defendant has access to information regarding the individuals affected by the Data Breach, and IMS has already provided notifications to some or all of those people on Defendant's behalf. Using this information, the members of the Class can be identified, and their contact information ascertained for purposes of providing notice.

189. **Particular Issues:** Particular issues are appropriate for certification under Rule 23(c)(4) because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the following:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members their Private Information had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members; and

i. Whether Class Members are entitled to actual, consequential, statutory, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

190. **Policies Generally Applicable to the Class:** Finally, class certification is also appropriate under Rule 23(b)(2) and (c). The Class is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward Class Members and making final injunctive relief appropriate with respect to each of the

Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly, and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

191. Defendant, through uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole, including without limitation the following:

h. Ordering Defendant to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members; and

i. Ordering that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain, and must require its vendors handling Private Information to implement and maintain, reasonable security and monitoring measures, including, but not limited to the following:

   i. prohibiting Defendant from engaging in the wrongful and unlawful acts alleged herein;

   ii. requiring Defendant to obligate and ensure its vendors protect, including through encryption, all data collected by Defendant and shared with its vendors through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

   iii. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' Private Information;

   iv. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks,

penetration tests, and audits on Defendant's vendors' systems on a periodic basis;

v. prohibiting Defendant from allowing its vendors to maintain Private Information on a cloud-based database until proper safeguards and processes are ensured;

vi. requiring Defendant to obligate its vendors to segment data by creating firewalls and access controls so that, if one area of their network is compromised, hackers cannot gain access to other portions of their systems;

vii. requiring Defendant to obligate its vendors to conduct regular database scanning and securing checks;

viii. requiring Defendant to obligate its vendors to monitor ingress and egress of all network traffic;

ix. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor its vendors' networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated;

x. requiring Defendant to meaningfully educate all Class Members about the threats that they because of the loss of their confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves; and

xi. incidental retrospective relief, including but not limited to restitution.

VI. CAUSES OF ACTION

COUNT I: NEGLIGENCE/NEGLIGENCE *PER SE*
(On behalf of Plaintiff and the Class)

192. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 172 above as if fully set forth herein.

193. Defendant required Plaintiff and Class Members to submit, directly or indirectly, personal, confidential Private Information to Defendant and its vendor IMS as a condition of receiving insurance coverage and related services.

194. Plaintiff and Class Members provided certain Private Information to Defendant and, through Defendant, to IMS, including their names, Social Security numbers, and other sensitive information.

195. Defendant had full knowledge of the sensitivity of the Private Information to which it were entrusted, and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information was wrongfully disclosed to unauthorized persons.

196. Defendant had duties to Plaintiff and each Class Member to exercise reasonable care in holding, using, sharing, safeguarding, and protecting their Private Information, including requiring and ensuring its vendors handling Private Information had reasonable and appropriate data security measures and policies in place to do so.

197. Plaintiff and Class Members were the foreseeable victims of any inadequate safety and security practices by Defendant or its service provider IMS.

198. Plaintiff and Class Members had no ability to protect their Private Information in Defendant's care or IMS's possession.

199. By collecting and storing Plaintiff's and Class Members' Private Information, Defendant had a duty of care to use reasonable means to secure and safeguard it, to prevent disclosure of the information, and to safeguard the Private Information from theft.

200. Defendant's duty of care obligated it to require and ensure that its vendor IMS provided data security data security consistent with industry standards and legal and regulatory requirements, and that IMS's systems and networks and the personnel responsible for them

adequately protected Plaintiff's and Class Members' Private Information.

201. Defendant's duty of care further obligated it to ensure its vendor IMS's processes to detect compromises of Private Information were sufficient.

202. Defendant was able to ensure IMS's systems and data security procedures were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a cybersecurity event like this Data Breach, whereas Plaintiff and Class Members were not.

203. Defendant had a duty to employ reasonable security measures under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

204. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PHI.

205. Defendant breached their duties to Plaintiff and Class Members under the FTC Act by failing to require, through contract or oversight, that its service provider IMS provided fair, reasonable, and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information, by failing to ensure the Private Information on IMS's system was encrypted and timely deleted when no longer needed, and by failing to provide notice to Plaintiff and Class Members of the Data Breach until nearly a year after it was discovered.

206. Defendant's violations of the FTC Act as described herein directly caused and/or were a substantial factor in the Data Breach and resulting injuries to Plaintiff and Class Members.

207. Plaintiff and Class Members are within the class of persons the FTC Act was intended to protect.

208. The type of harm that resulted from the Data Breach was the type of harm the FTC

Act was intended to guard against.

209. Defendant's failures to comply with the FTC Act is negligence *per se.*

210. Defendant's duty to use reasonable care in protecting Plaintiff's and Class Members' Private Information arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to secure such Private Information.

211. Defendant breached its duties and was negligent by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information from unauthorized disclosure in the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to require and periodically ensure that its vendor IMS adopted, implemented, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Private Information;

b. Failing to adequately monitor the security of IMS's information technology networks and systems;

c. Failure to require and periodically ensure that IMS's network systems had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Plaintiff's and Class Members' Private Information; and

e. Failing to timely notify Plaintiff and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

212. But for Defendant's wrongful and negligent breaches of its duties owed to Plaintiff

and Class Members, the Data Breach would not have occurred or at least would have been mitigated, Plaintiff's and Class Members' Private Information would not have been compromised, and Plaintiff's and Class Members' injuries would have been avoided.

213. It was foreseeable that Defendant's failures to use reasonable measures to protect Plaintiff's and Class Members' Private Information would injure Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable to Defendant given the known high frequency of cyber-attacks and data breaches in Defendant's industry.

214. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' Private Information would cause them one or more types of injuries.

215. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injuries and damages, including but not limited to (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) actual identity theft and fraud; (d) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (e) loss of benefit of their bargain; and (f) the continued and certainly increased risk to their Private Information, which remains (i) unencrypted and available for unauthorized third parties to access and abuse; and (ii) in Defendant's control and IMS's possession and subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect it.

216. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injuries and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

217. Plaintiff and Class Members are entitled to damages, including compensatory,

punitive, and nominal damages, in an amount to be proven at trial.

COUNT II: BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Nationwide Class)

218. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 172 above as if fully set forth herein.

219. Defendant required Plaintiff and Class Members to provide and entrust their Private Information to Defendant as a condition of obtaining insurance and/or benefit products and services from Defendant.

220. When Plaintiff and Class Members provided their Private Information to Defendant, they entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such Private Information and to timely and accurately notify Plaintiff and Class Members if and when their Private Information was breached and compromised.

221. Specifically, Plaintiff and Class Members entered into valid and enforceable implied contracts with Defendant when they agreed to provide their Private Information and/or payment to Defendant.

222. The valid and enforceable implied contracts that Plaintiff and Class Members entered into with Defendant included Defendant's promises to protect Private Information it collected from Plaintiff and Class Members, or created on its own, from unauthorized disclosures. Plaintiff and Class Members provided this Private Information in reliance on Defendant's promises.

223. Under the implied contracts, Defendant promised and was obligated to (a) provide insurance and/or benefits products and services to Plaintiff and Class Members; and (b) protect Plaintiff's and Class Members' Private Information provided to obtain such services and/or created in connection therewith. In exchange, Plaintiff and Class Members agreed to provide Defendant

with payment and their Private Information.

224. Defendant promised and warranted to Plaintiff and Class Members, including through its public-facing Privacy Notice identified above, to maintain the privacy and confidentiality of the Private Information it collected from Plaintiff and Class Members and to keep such information safeguarded against unauthorized access and disclosure.

225. Defendant's adequate protection of Plaintiff's and Class Members' Private Information was a material aspect of these implied contracts with Defendant.

226. Defendant solicited and invited Plaintiff and Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

227. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with industry standards and relevant laws and regulations, including the FTC Act.

228. Plaintiff and Class Members who contracted with Defendant for insurance and/or benefit products and services and provided their Private Information to Defendant reasonably believed and expected that Defendant would adequately employ adequate data security to protect that Private Information. Defendant failed to do so.

229. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their Private Information to Defendant and agreed Defendant would receive payment for, amongst other things, the protection of their Private Information.

230. Plaintiff and Class Members performed their obligations under the contracts when they provided their Private Information and/or payment to Defendant.

231. Defendant materially breached its contractual obligations to protect the Private

Information it required Plaintiff and Class Members to provide when that Private Information was unauthorizedly disclosed in the Data Breach due to Defendant's inadequate data security measures and procedures.

232. Defendant materially breached its contractual obligations to deal in good faith with Plaintiff and Class Members when it failed to take adequate precautions to prevent the Data Breach and failed to promptly notify Plaintiff and Class Members of the Data Breach.

233. Defendant materially breached the terms of its implied contracts, including but not limited to by failing to comply with industry standards or the standards of conduct embodied in statutes like Section 5 of the FTC Act, by failing to otherwise protect Plaintiff's and Class Members' Private Information, and/or by failing to prevent the same data security failures by its vendor IMS that handled Private Information, as set forth *supra*.

234. The Data Breach was a reasonably foreseeable consequence of Defendant's conduct, by acts of omission or commission, in breach of these implied contracts with Plaintiff and Class Members.

235. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Class Members did not receive the full benefit of their bargains with Defendant, and instead received services of a diminished value compared to that described in the implied contracts. Plaintiff and Class Members were therefore damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and that which they received.

236. Had Defendant disclosed that its data security procedures were inadequate or that it and its vendor did not adhere to industry-standard for cybersecurity, neither Plaintiff, Class Members, nor any reasonable person would have contracted with Defendant.

237. Plaintiff and Class Members would not have provided and entrusted their Private Information to Defendant in the absence of the implied contracts between them and Defendant.

238. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

239. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their Private Information and by failing to provide timely or adequate notice that their Private Information was compromised in and due to the Data Breach.

240. As a direct and proximate result of Defendant's breach of its implied contracts with Plaintiff and Class Members and the attendant Data Breach, Plaintiff and Class Members have suffered injuries and damages as set forth herein and have been irreparably harmed, as well as suffering and the loss of the benefit of the bargain they struck with Defendant.

241. Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or restitution, in an amount to be proven at trial.

242. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (a) strengthen its data security systems and monitoring procedures; (b) conduct annual audits of its vendor's data security systems and monitoring procedures; and (c) provide adequate lifetime credit monitoring to all Class Members.

COUNT III: INVASION OF PRIVACY/INSTRUSION UPON SECLUSION
(On behalf of Plaintiff and the Nationwide Class)

243. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 172 above as if fully set forth herein.

244. Plaintiff and Class Members had a legitimate expectation of privacy to their Private Information and were entitled to Defendant's protection of this Private Information in its control against disclosure to unauthorized third parties.

245. Defendant owed a duty to its customers, including Plaintiff and Class Members, to keep their Private Information confidential and secure.

246. Defendant failed to protect Plaintiff's and Class Members' Private Information and instead caused it to be accessed and exposed to unauthorized persons, a notorious ransomware group, which has already made the Private Information publicly available and disseminated it to thousands of people, including through publishing the data on its dark web leak site, where cybercriminals go to find their next identity theft and extortion victims.

247. Defendant allowed unauthorized third parties access to and examination of the Private Information of Plaintiff and Class Members, by way of Defendant's failure to protect the Private Information through reasonable data security measures.

248. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiff and Class Members is highly offensive to a reasonable person and represents an intrusion upon Plaintiff's and Class Members' seclusion as well as a public disclosure of private facts.

249. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their Private Information to Defendant as a condition of and in exchange for receiving insurance and/or benefits products and services, but privately with an intention that the Private Information would be kept confidential and protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

250. Subsequent to the intrusion, Defendant permitted Plaintiff's and Class Members' data to be published online to countless cybercriminals whose mission is to misuse such information, including through identity theft and extortion.

251. The Data Breach constitutes an intentional or reckless interference by Defendant with Plaintiff's and Class Members' interests in solitude or seclusion, as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

252. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur, because it had actual knowledge that its diligence and oversight of its vendors' information security practices were inadequate and insufficient to protect Plaintiff' and Class Members' Private Information from unauthorized disclosure.

253. Defendant acted with reckless disregard for Plaintiff' and Class Members' privacy when it caused their Private Information to be shared, used, and stored by IMS without adequate protections, including encryption, allowing LockBit to access and take Plaintiff's and Class Members' Private Information in the Data Breach.

254. Defendant was aware of the potential of a data breach and failed to adequately vet, audit, or oversee its vendor IMS's network systems or implement appropriate policies to prevent the unauthorized release of Plaintiff' and Class Members' Private Information to cybercriminals.

255. Because Defendant acted with this knowing state of mind, it had notice and knew that its inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

256. As a direct and proximate result of Defendant's acts and omissions set forth above, Plaintiff' and Class Members' Private Information was disclosed to third parties without authorization, causing Plaintiff and Class Members to suffer injuries and damages including, without limitation, (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) out-of-pocket and lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) loss of benefit of the

bargain; and (e) the continued and certainly increased risk to their Private Information, which remains in Defendant's control and its vendors' possession in unencrypted form and subject to further unauthorized disclosures, so long as Defendant fails to undertake appropriate and adequate measures to protect it.

257. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the Private Information maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members.

COUNT IV: UNJUST ENRICHMENT
(On behalf of Plaintiff and the Nationwide Class)

258. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 172 above as if fully set forth herein.

259. This count is brought in the alternative to the breach of implied contract count above.

260. Plaintiff and Class Members conferred a benefit on Defendant by way providing, directly or indirectly, payment and their Private Information to Defendant as part of Defendant's business.

261. Defendant required Plaintiff's and Class Members' Private Information to conduct and facilitate its business and generate revenue, which it could not do without collecting, using, and sharing with IMS Plaintiff's and Class Members' Private Information.

262. The monies paid to Defendant included a premium for Defendant's cybersecurity obligations and were supposed to be used by Defendant, in part, to pay for the administrative and

other costs of providing reasonable data security and protection for Plaintiff's and Class Members' Private Information.

263. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class Members by hiring vendors with cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

264. Defendant failed to provide reasonable security, safeguards, and protections to the Private Information of Plaintiff and Class Members, and as a result, Defendant was overpaid.

265. Under principles of equity and good conscience, Defendant should not be permitted to retain the money because it failed to provide adequate safeguards and security measures to protect Plaintiff's and Class Members' Private Information, which Plaintiff and Class Members paid for but did not receive.

266. Defendant wrongfully accepted and retained these benefits—payment and Plaintiff's and Class Members' Private Information—and was enriched to the detriment of Plaintiff and Class Members.

267. Defendant's enrichment at Plaintiff's and Class Members' expense is unjust.

268. As a result of Defendant's wrongful conduct and resulting unjust enrichment, Plaintiff and Class Members are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by Defendant, plus reasonable attorneys' fees and costs.

COUNT V: DECLARATORY JUDGMENT
(On behalf of Plaintiff and the Nationwide Class, or alternatively, on behalf of the State SubClass, against all Defendant)

269. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 172 above as if fully set forth herein.

270. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary supplemental relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

271. In the fallout of the Data Breach, a controversy has arisen about Defendant's duties to use reasonable data security for the Private Information it collects, uses, shares, and maintains.

272. On information and belief, Defendant's actions were—and *still* are—inadequate and unreasonable. Plaintiff and Class Members continue to suffer injuries from the ongoing threat of fraud and identity theft due to Defendant's inadequate data security measures.

273. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring as follows:

a. Defendant owed—and continue to owe—a legal duty to use reasonable data security to secure the Private Information entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendant breached, and continue to breach, its duties by failing to use reasonable measures to protect the Private Information entrusted to it from unauthorized access, use, and disclosure; and

d. Defendant's breaches of its duties caused—and continues to cause—injuries to Plaintiff

and Class Members.

274. The Court should also issue injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the Private Information entrusted to it.

275. That Defendant's service provider was previously the target of one of a devastating data breach, yet Defendant still refused to act proactively to prevent the exposure of thousands of individuals' Private Information in this Data Breach through improved data security vetting, auditing, and supervision measures, like thorough due diligence and oversight of its vendors handling Private Information, highlights the need for an injunction here—lest Defendant continue to skimp on cybersecurity to augment its own profits while leaving individuals like Plaintiff and Class Members to suffer the consequences.

276. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injuries and lack an adequate legal remedy if Defendant's vendor(s) experiences another data breach. And if another breach occurs, Plaintiff and Class Members will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full, and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted for out-of-pocket damages and other legally quantifiable and provable damages, cannot cover the full extent of Plaintiff's and Class Members' injuries.

277. If an injunction is not issued, the resulting hardship to Plaintiff and Class Members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

278. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class Members, and the public at large.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, prays for

judgment as follows:

A. An Order certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

B. Awarding Plaintiff and the Class damages that include applicable compensatory, actual, statutory, nominal, exemplary, and punitive damages, as allowed by law;

C. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

D. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

E. Awarding injunctive relief in the form of additional technical and administrative cybersecurity controls as is necessary to protect the interests of Plaintiff and the Class;

F. Enjoining Defendant from further deceptive practices and making untrue statements about its data security, the Data Breach, and the transmitted Private Information;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law; and

I. Awarding such further relief to which Plaintiff and the Class are entitled.

VIII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues to triable.

Dated: September 13, 2024

Respectfully submitted,

/s/ Steven Sukert

Steven Sukert, NY Bar No. 5690532
Jeff Ostrow*
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd, Suite 500
Fort Lauderdale, FL 33301

Tel: (954) 525-4100
Fax: (954) 525-4300
sukert@kolawyers.com
ostrow@kolawyers.com

J. Gerard Stranch, IV *
Grayson Wells*
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
(615) 254-8801
gstranch@stranchlaw.com
gwells@stranchlaw.com

*Motion for *Pro Hac Vice* Admission forthcoming

Counsel for Plaintiff and the Proposed Class